UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,223	08/16/2001	Thomer Michael Gil	12221-007001	2855

26161 7590 03/24/2005

FISH & RICHARDSON PC
225 FRANKLIN ST
BOSTON, MA 02110

EXAMINER	
NGUYEN, TRONG NHAN P	
ART UNIT	**PAPER NUMBER**
2152	

DATE MAILED: 03/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,223	GIL ET AL.	
	Examiner	Art Unit	
	Jack P Nguyen	2152	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-49* is/are pending in the application.

4a) Of the above claim(s) *22-49* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *1/31/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to applicant's election to a restriction requirement received on 12/22/04. Applicant elected Group I that includes claims 1-21 without traverse. Claims 22-49 are withdrawn. Claims 1-21 are now being examined.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carlson, 6,381,649 (Carlson hereafter) in view of Woo, US Pub 2002/0023089 (Woo hereafter).

As per claim 21, Carlson discloses a data monitoring and analyzing computing system that collect statistical information about network flows (abstract; col. 6, lines 38-41) comprising: a computing device that executes a computer program product stored on the computer readable medium comprising instructions to cause the computing device to (11, fig. 1; col. 5, lines 5-9; switching node 'SN' computer is the computing device that performs the data monitoring and analyzing); monitors and collects traffic flow data (i.e, accumulates packets statistics) and stores the traffic data into memory locations known as buckets (col. 7, lines 46-51; monitoring device has memory

locations called buckets to store traffic packet data); compare the accumulated statistic values (network flow data) from the buckets to configured threshold values corresponding to the number of buckets to determine that an event is of significance (col. 3, lines 40-46; col. 7, lines 32-36 & 55-65; monitoring device compares the data units in the buckets to predetermined threshold values; out of compliance packets are 'marked' for discarding to prevent the system from excess network traffic or traffic congestion); a port to link the data collector to a central control center (20, fig. 2; col. 6, lines 38-43; input module (20, fig. 2) port links the monitoring and data collecting mechanism to the switching node (or central control device). Carlson does not explicitly disclose using a hash function to map traffic flow (packets) into the buckets and adjusting the number of buckets as the number of buckets approaches a threshold (or some pre-determined value). In an analogous art to the claimed invention, Woo discloses a packet filtering system using a hashing function to search for the packets in the index bucket table (page 5, paragraphs 0093, 0096, 0098; packet data is mapped using hash function in the index table (30, fig. 2); adjusting the number of bucket filters as the packet data reaches a pre-specified (threshold) value (page 1, paragraph 0023; page 4, paragraphs 0080, 0081; as the number of packets reaches a threshold value, the number of filter buckets can change dynamically). Hence, it would have been obvious to one of ordinary skill in the art to modify and combine the teachings of Carlson and Woo to use a hash function for quick sorting or lookup and adjusting the number of buckets (or filters) to accommodate changing traffic conditions as desired by the user as disclosed by Woo on [page 5, paragraph 0091].

Claims 1 and 14 recite similar limitations to claim 21; therefore, they are rejected using similar rationale as claim 21.

As per claims 2 and 19, Carlson discloses the buckets are storage areas in a memory space of the monitor device (col. 7, lines 46-51).

As per claim 3, Carlson discloses as the number of buckets changes, the buckets have values derived from the buckets prior to the change (col. 7, lines 49-54; system stores data in plurality of buckets; system maintains values of each bucket).

As per claims 4 and 17, Woo discloses using hash function to map data in the all the buckets (see claim 21 rejection; data mapping using hash function applies to new buckets as well).

As per claim 5, Carlson discloses comparing the value accumulated in the bucket to a threshold that depends on the number of buckets (col. 7, lines 32-36).

As per claims 6 and 18, Carlson discloses the parameter is the count of how many packets a data collector examines (col. 4, lines 7-9; counter is used to keep track of number of data units being stored in a bucket).

As per claim 7, Carlson discloses a parameter for one bucket approaches a threshold, the monitoring device raises an alarm (col. 3, lines 43-46; when the value exceeds a predetermined threshold, the system raises the alarm by 'marking' the packets to let the system administrator know that the traffic is out of compliance).

As per claims 8 and 20, Woo discloses applying security measures to the packet filtering system to prevent various unauthorized accesses (page 10, paragraph 0201; packets are classified by VPN or tunnel filters). Even if Woo does not explicitly disclose

changing the hashing function periodically so that packets are reassigned to different buckets, it would have been obvious to one of ordinary skill in the art to apply various security measures to prevent the system from unauthorized access or network attacks from intruders.

As per claims 9-10, Carlson discloses the data monitoring system dynamically collects and divides traffic flow data into variable number of buckets over a variable of memory locations as desired and compare the values against predetermined thresholds to determined if the traffic flow is out of compliance (see claim 23). Carlson further discloses discarding the 'marked' packets if the system deems those packets are causing denial of service attacks (i.e., by causing excess data traffic or traffic congestion) against its own network (col. 3, lines 40-46).

As per claim 11, Carlson discloses the traffic is monitored at multiple levels of granularity, from aggregate to individual flows (col. 6, lines 37-41; data packets (most granular component of data flow) are being monitored by monitoring device to keep the network from intruders or out of compliance; streams of data that are out of compliance are 'marked' for discarding).

As per claim 12, Carlson discloses the traffic is applied to monitoring of TCP packet ratios and repressor traffic (col. 5, lines 37-38; col. 3, lines 40-46; out of compliance packets are 'marked' for discarding when they pose a threat to the network).

As per claim 13, Carlson discloses comparing accumulated statistic values from the buckets to second threshold values to determine that an event is of significance (col. 3, lines 40-46; col. 7, lines 32-36 & 55-65; monitoring device compares the data units in

the buckets to predetermined threshold values; out of compliance packets are 'marked' for discarding to prevent the system from excess network traffic or traffic congestion);

As per claims 15-16, Carlson discloses based on the second threshold, the buckets are divided into more buckets (col. 7, lines 46-54; data flows can be separated and stored in plurality of 'buckets' as desired when a predetermined units of data threshold is reached in each bucket; data in each bucket is related to (or derived from) each other).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Jones, 5,796,956; Plevyak et al, 6,848,005; Aubert et al, 6,388,992; Giroux et al, 6,370,116; Bar et al, 6,807,667; Hughes et al, 6,535,484; Schuba et al, 6,725,378

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jack P Nguyen whose telephone number is (571) 272-3945. The examiner can normally be reached on M-F 8:30-5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenton Burgess can be reached on (571) 272-3949. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

jpn

Dung C. Dinh
Primary Examiner